

### **REMARKS**

The Examiner rejected claims 5, 10 and 19-30 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Vaidya (US Patent Number 6,279,113) in view of Sharma *et al.* (US Patent Number 6,909,692) hereinafter referred to as Sharma.

The Examiner rejected claims 6 and 11 under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Vaidya and Sharma as applied to claims 5 and 10 above respectively, and further in view of Lunt (Detecting Intruders in Computer Systems).

The Examiner rejected claims 7 and 12 under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Vaidya and Sharma as applied to claims 5 and 10 above respectively, and further in view of Martin *et al.* (US Patent Number 6,772,349) hereinafter referred to as Martin.

Applicants respectfully traverse the § 103 rejections with the following arguments.

**35 U.S.C. §103(a)**

The Examiner rejected claims 5, 10 and 19-30 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Vaidya (US Patent Number 6,279,113) in view of Sharma *et al.* (US Patent Number 6,909,692) hereinafter referred to as Sharma.

Applicants respectfully contend that claims 5 and 10 are not unpatentable over Vaidya in view of Sharma, because Vaidya in view of Sharma does not teach or suggest each and every feature of claims 5 and 10.

As a first example of why , Vaidya in view of Sharma does not teach or suggest the feature: **“for each occurrence of the value of the signature event counter exceeding the signature threshold quantity: generating an alert by an intrusion detection sensor of the intrusion detection system, recording a time of generating the alert in a log of a governor , comprised by the intrusion detection sensor, determining from contents of the log a present alert generation rate, and comparing the present alert generation rate with an alert generation rate threshold”** (emphasis added).

The Examiner argues that Sharma teaches “Sharma teaches that generating too many alerts in a network management system can crash the system (See Sharma Col. 3 Paragraph 3) and further teaches that in order to control the alert generation rate, each alert should be logged including a time of the alert (See Sharma Col. 8 Line 61 – Col. 9 Line 15), an alert generation rate should be determined using the log (See Sharma Col. 9 Lines 16-25), the determined rate should be compared with a threshold (See Sharma Col. 9 Lines 25-27)”.

In response, Applicants agree with the Examiner that Sharma teaches “recording a time of generating the alert in a log of a governor comprised by the intrusion detection sensor, determining from contents of the log a present alert generation rate, and comparing the present alert generation rate with an alert generation rate threshold”.

However, claims 5 and 10 require performance of:

“generating an alert by an intrusion detection sensor of the intrusion detection system”

AND

“recording a time of generating the alert in a log of a governor comprised by the intrusion detection sensor, determining from contents of the log a present alert generation rate, and comparing the present alert generation rate with an alert generation rate threshold”

FOR EACH OCCURRENCE OF

“the value of the signature event counter exceeding the signature threshold quantity”.

Thus, claims 5 and 10 require that **for each occurrence of the value of the signature event counter exceeding the signature threshold quantity**: “generating an alert” occurs and the “recording”, “determining”, and “comparing” steps also occur. Therefore, whenever “generating an alert” is performed, the “recording”, “determining”, and “comparing” (i.e., “comparing the present alert generation rate with an alert generation rate threshold”) steps are also performed.

Applicants acknowledge that Sharma teaches performing the “recording” step whenever the step of “generating an alert” is performed”. However, Sharma does not teach performing the “determining” and “comparing” steps whenever the step of “generating an alert” is performed”.

To the contrary, Sharma, col. 9, lines 16-20 teaches that the “determining” and “comparing” steps are performed only after the step of “generating an alert” is performed” approximately 1000 times.

The preceding limitation of claims 5 and 10 are illustrated in FIG. 4 of the present patent application, which shows the “generating”, “recording”, “determining”, and “comparing” steps 415, 420, 440, and 450, respectively, all occurring in each iteration of the loop triggered by the “Threshold Exceeded” decision step.

Accordingly, claims 5 and 10 are not unpatentable over Vaidya in view of Sharma.

Based on the preceding arguments, Applicants respectfully maintain that claim 5 is not unpatentable over Vaidya in view of Sharma, and that claim 5 is in condition for allowance. Since claims 19-24 depend from claim 5, Applicants contend that claims 19-24 are likewise in condition for allowance. Since claims 25-30 depend from claim 10, Applicants contend that claims 25-30 are likewise in condition for allowance.

In addition with respect to claims 24 and 30, Vaidya in view of Sharma does not teach or suggest the feature: **“wherein for each occurrence of the value of the signature event counter exceeding the signature threshold quantity: after generating the alert and before determining from contents of the log the present alert generation rate, the method further comprises the step of: clearing the log of any entries that are past a specified age”** (emphasis added).

The Examiner argues: “Regarding claims 24 and 30, Vaidya and Sharma disclosed that after generating the alert and before determining from contents of the log the present alert

generation rate, the method further comprises the step of: clearing the log of any entries that are past a specific age (See Sharma Col. 9 Paragraph 2 and Vaidya Col. 12 Paragraph 2 wherein Vaidya disclosed purging the expired entries of a log prior to determining the generation rate associated with the log).”

In response, Applicants respectfully contend that Vaidya, col. 12, Par. 2 does not disclose: (1) that the purging occurs “for each occurrence of the value of the signature event counter exceeding the signature threshold quantity”; (2) that the purging occurs “after generating the alert and before determining from contents of the log the present alert generation rate”; and (3) that the generation rate is associated with the log (in consideration of the fact that the “log” in Vaidya, col. 12, Par. 2 is allegedly the state cache 44 and Vaidya does not disclose that a generation rate is associated with the entries in the state cache 44).

Therefore, Vaidya in view of Sharma does not teach or suggest the preceding feature of claims 24 and 30.

The Examiner rejected claims 6 and 11 under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Vaidya and Sharma as applied to claims 5 and 10 above respectively, and further in view of Lunt (Detecting Intruders in Computer Systems).

Since claims 6 and 11 respectively depend from claims 5 and 10, which Applicants have argued *supra* to not be unpatentable over Vaidya in view of Sharma under 35 U.S.C. §103(a), Applicants maintain that claims 6 and 11 are likewise not unpatentable over Vaidya in view of Sharma and further in view of Lunt under 35 U.S.C. §103(a).

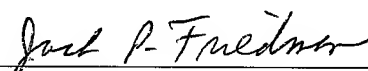
The Examiner rejected claims 7 and 12 under 35 U.S.C. § 103(a) as allegedly being unpatentable over the combination of Vaidya and Sharma as applied to claims 5 and 10 above respectively, and further in view of Martin *et al.* (US 6,772,349) hereinafter referred to as Martin.

Since claims 7 and 12 respectively depend from claims 5 and 10, which Applicants have argued *supra* to not be unpatentable over Vaidya in view of Sharma under 35 U.S.C. §103(a), Applicants maintain that claims 7 and 12 are likewise not unpatentable over Vaidya in view of Sharma and further in view of Martin under 35 U.S.C. §103(a).

### CONCLUSION

Based on the preceding arguments, Applicants respectfully believe that all pending claims and the entire application meet the acceptance criteria for allowance and therefore request favorable action. If the Examiner believes that anything further would be helpful to place the application in better condition for allowance, Applicants invites the Examiner to contact Applicants' representative at the telephone number listed below. The Director is hereby authorized to charge and/or credit Deposit Account No. 09-0457.

Date: 11/08/2006

  
\_\_\_\_\_  
Jack P. Friedman  
Registration No. 44,688

Schmeiser, Olsen & Watts  
22 Century Hill Drive - Suite 302  
Latham, New York 12110  
(518) 220-1850